HP iPAQ Handheld Security Solutions

Overview

Protecting the private information on your HP iPAQ is serious business. There are many ways that you can protect your HP iPAQ. Taking advantage of the built-in security features is a great way to start protecting your HP iPAQ. These security features are powerful defenses against data theft. Your login name and password are great ways to begin protecting your HP iPAQ against theft. It is important to protect the information contained on your HP iPAQ from unauthorized access. Data encryption is probably the best way to protect information on mobile devices as well as on external storage cards. (Data encryption is a conversion process that is used for protecting data.)

This white paper provides detailed information about HP ProtectTools, Odyssey Client®, and biometric security solutions. In today's world, a lot of valuable information is being stored on handheld devices. That is why securing your personal data is so important to HP. The HP ProtectTools security features provide on-device security protection that decreases the risk of you losing sensitive data and from unauthorized access on your HP iPAQ. In addition, Odyssey Client allows easy and secure connection to a wireless network. This document is designed to assist you in understanding security and how it works on HP iPAQ devices.

Security

Security is a crucial issue facing business users today. Without strong security protection, a lost or stolen mobile device can give unauthorized users easy access to mission-critical data and network resources, exposing the business to potential legal liability, financial loss, and competitive espionage.

For these reasons, strong security is an indispensable asset for mobile business computing devices such as HP iPAQ handhelds. HP iPAQ devices address these security challenges head-on with a unique mix of advanced features and tools designed to prevent unauthorized access to user data. Several important technologies converge to make it happen:

- HP ProtectTools secured by CREDANT Technologies uses many of the same capabilities found in that company's enterprise-class Mobile Guardian® product, including user authentication and data encryption. (Authentication is the process of granting or denying someone access to a network resource.)
- Odyssey Client developed by Funk Software, Inc. allows users to connect their device (HP iPAQ hw6900 Mobile Messenger series only) to multiple secured wireless networks. Odyssey Client supports networks that adhere to the 802.11b wireless LAN standards. These networks can be found in hotels, airports, and other Internet hotspots.
- A special Biometric Fingerprint Reader allows users to easily login with a swipe of the finger (HP iPAQ hx2700 series Pocket PC only) and/or with a PIN (personal identification number). This feature provides highly secure, convenient, and fast authentication—without users having to remember passwords.
- Full virtual private network (VPN) and WEP-enhanced security is included in the Microsoft operating system. A VPN provides enhanced security when accessing corporate data over the Internet. WEP provides 64-bit and 128-bit encryption security when connected via wireless networks (802.11b).
- Even more advanced security for wireless communication through built-in support for 802.1X and WPA (Wi-Fi Protected Access) along with support for LEAP and TKIP. LEAP is used for authentication purposes.

Mobile viruses are not currently a serious threat; but, it is important be aware of potential risks to your HP iPAQ. Viruses (also called worms or Trojan horses) are malicious and can be widely distributed. When you download programs or files that are already infected, a virus can spread between your personal computer, laptop, or other removable storage. To get more information about mobile viruses, visit http://www.microsoft.com/athome/security/viruses/mobilevirus.mspx.

HP ProtectTools

The special security technology found in many HP iPAQ devices is provided by HP ProtectTools, a suite of built-in, not bolted on security solutions. These security solutions are based on the same technologies used by market leader CREDANT Technologies Inc. CREDANT Mobile Guardian® (CMG) provides solutions that reduce specific security risks to handheld users. These security solutions provide certain advantages that allow you to protect your device more effectively. The first layer of security involves PIN or password access for HP iPAQ devices. A second layer of defense involves data encryption, which helps ensure that sensitive information remains confidential.

You can encrypt e-mail messages, attachments, My Documents, and other files that are then automatically protected whether stored on the device or an external storage card.

(By default, all data in the My Documents folder is encrypted.) If you forget your PIN or password, you can regain access by entering an answer to a pre-selected question.

If a device is lost or stolen, aggressive failsafe actions can be automatically invoked to hard reset the device back to factory defaults after a pre-determined number of access attempts.

Using HP ProtectTools

HP ProtectTools helps protect your device and the data stored on it. When HP ProtectTools is enabled, you may have an option to enroll a fingerprint or enter a PIN and/or password to access the device.

Once you have set the security features on your device and are unable to successfully swipe your fingerprint or forget your PIN or password, you can access your device with a back-up question and answer.

You should only need to set up HP ProtectTools one time. If needed, you can make changes to any of your security settings later.

Refer to the HP iPAQ documentation on the *Companion* CD or *Getting Started* CD to learn more about:

- Setting up HP ProtectTools
- Managing security options
- Changing your HP ProtectTools settings
- Encrypting/decrypting data

Odyssey Client

Using Odyssey Client, you can do the following:

- Connect your HP iPAQ to a wireless network
- Connect peer-to-peer to other devices on a network
- Configure multiple networks to connect to various networks (possibly using different credentials and/or authentication methods)
- Use 802.1x to authenticate to a network
- Use various authentication methods (such as EAP-TTLS, EAP-PEAP, and EAP-TLS protocols) to keep your credentials secure

To use Odyssey Client on your HP iPAQ, your device must have an 802.1x-compliant (network interface card) NIC driver. The HP iPAQ can be compatible with your preferred WLAN security protocol for network authentication. A *readme.txt* file is included with the Odyssey Client software that lists compatible devices.

You will need a license key to use Odyssey Client. A license key is a text sequence that corresponds to your licensed copy of Odyssey Client. During the installation process, you are prompted to enter the license key.

You can also enter the license key after the installation process. Several features of Odyssey Client are licensed separately. Depending on the license, some features may be unavailable and areas of the user interface may be grayed out.

You will need to install the Odyssey Client software onto your HP iPAQ. For instructions on installing Odyssey Client via the CD or web download version, refer to the information that came with your HP iPAQ.

After configuring a network on Odyssey Client, you must be within range of an access point to log on to a specified network and connect to it. Some wireless networks require that you log on while others let anyone within range log on. The access point links your HP iPAQ to a network. (The range of an access point is usually several hundred feet.) If there is no access available, two or more wireless devices can use peer-to-peer networking to share files and play games. No additional hardware equipment is needed to use peer-to-peer networking.

Currently, the Odyssey Client for network authentication is available with the HP iPAQ hw6900 Mobile Messenger series only.

Biometric Fingerprint Reader (HP iPAQ hx2700 series only)

The built-in Biometric Fingerprint Reader is exclusive to the HP iPAQ hx2700 series. The built-in fingerprint reader is convenient, and it adds an extra level security for authorized users. This robust security feature easily identifies authorized users and prevents access by others. Depending on the strength of protection required, you can specify whether to identify yourself using only a fingerprint, a PIN, a password, or various combinations of these methods.

This type of identification is virtually foolproof, for the simple reason that fingerprints are a unique form of biometric identification possessed only by the specific user. This also provides the ultimate in convenient access and does not have to be remembered like a password or PIN.

You can also find more specific information about how to enroll fingerprints using HP ProtectTools in the *User's Guide* on the *Companion* CD. (If you purchased an HP iPAQ hx2700 Pocket PC, the *Companion* CD is available with your device.)

Special issues related to security

The unprecedented set of powerful security features found in the HP iPAQ hx2000 series requires new behavior for some individual users. In particular, users may find that they run the risk of losing current data in the devices if regular backups do not occur and they forget any required access passwords or PIN numbers. This is because a locked device without a password requires a "hard reset" that will wipe out all of the data on the unit.

The "hard reset" feature is another level of security that helps prevent data theft by unauthorized users. For the strongest level of protection, you can set a flag in the device that blocks any attempt to log back in after a certain number of tries. The HP default is to turn this flag off. If this flag is turned on, in circumstances where lockout occurs, there is no recovery from the lockout that will preserve your data.

Recovering from a locked device

If the device locks and you enter a correct answer to the pre-selected question, this regains access to the device and its data. If you forget the PIN/password and the answer to the preselected question, there is no way to recover from a locked device without losing data. The device will prompt for a hard or clean reset, and all memory will be set back to the default factory condition which includes deleting data in the iPAQ File Store. If this option is chosen, the iPAQ File Store takes more than 10 minutes to initialize. During this initialization process, it is recommended that you connect your HP iPAQ to AC power to avoid timeouts.

However, if you forget your PIN, but successfully enter your hint question/answer, you are prompted to enter a new PIN. If you do not answer the hint question/answer successfully, there is a time delay between the hint question/answer attempts until you enter the correct answer.

Passphrases

When HP ProtectTools is initiated, you are prompted for a passphrase that is different than the PIN or password used to access the device. The passphrase is created for one reason: if data is stored on a memory card and encrypted by HP ProtectTools, a passphrase is used to facilitate sharing the data with other HP iPAQ devices. In other words, HP iPAQ devices that use the same passphrase can also share the data that is encrypted on memory cards.

One special example occurs when HP ProtectTools is disabled but data is still encrypted on a memory card. This data can be retrieved from the card if HP ProtectTools is reinitiated on the HP iPAQ using the same passphrase used previously when the data was encrypted on the card. Thus, like PINs and passwords, it is important to store the passphrase in a secure location. Passphrases must be at least eight characters long and must include at least one punctuation mark. For best results, a mix of at least 30 numbers, letters, and special characters should be used.

Performance considerations related to data encryption

With HP ProtectTools, the HP iPAQ automatically encrypts data stored on the device using one of four encryption algorithms. These encryption algorithms are listed below in order of the strongest to the weakest:

- Lite
- AES (advanced encryption standard)
- Blowfish
- 3DES

When you lock and unlock the device, the HP iPAQ encrypts and decrypts the data using whichever algorithm is chosen. Since the computer must run all data through this algorithm, the encryption/decryption operation will take time and affect the performance of the device.

If you have a large amount of data on your device and choose to encrypt it all, regardless of processor performance, it will take time to decrypt the data To improve performance, you may consider encrypting only the most critical data. Performance can also be improved somewhat by moving to weaker encryption algorithm. For instance, someone using AES for encryption can see a small performance improvement by changing to the Blowfish method, which is still strong but not quite as strong as AES. It is possible to change the encryption settings later, but this also involves a wait while the data is being converted from one format to the other.

Encrypting your personal data is the best way to protect your personal information. The encryption process runs in the background, so you are able to perform other tasks on your HP iPAQ during this time. There are two methods to monitor the decryption process. To find out more about encrypting and decrypting data, refer to the documentation on the *Companion* CD or *Getting Started* CD that came with your HP iPAQ.

Network Connections

You will need to configure the networks you want to connect to. Using your HP iPAQ, you must be within the range of the access point to initiate network authentication. You will need your logon credentials to access various networks: SSID, user name, password, and domain name. You will then be able to select an available network from an on-screen list.

To get specific information about configuring and logging on to networks, refer to the documentation that came with your HP iPAQ.

Virtual Private Network and Wired Equivalency Privacy

A virtual private network (VPN) allows two or more private networks to be connected over a publicly accessed network. Primarily, a VPN connection helps you to securely connect to servers (such as a corporate network) via the Internet. In a sense, VPNs are similar to WANs or a securely encrypted tunnel. The key feature of VPNs is that they can use public networks like the Internet rather than rely on expensive, privately leased lines.

Additionally, VPNs have the same security and encryption features as private networks. To learn more about setting up and connecting to a VPN, refer to the documentation on the *Companion* CD *or Getting Started* CD that came with your HP iPAQ.

Wired Equivalency Privacy (WEP) encrypts data immediately before wireless transmissions are sent, and decrypts data it receives. WEP is a security protocol designed to provide a wireless local area network (WLAN) with the same level of security usually expected on a local area network (LAN). Basically, WLAN is a wireless network in which a mobile user can connect to a local area network through a wireless connection.

WEP security is considered the first significant line of defense against casual eavesdroppers. If WEP uses a secret key, which is considered similar to a password, then the key must be available on all of the network's wireless devices. WEP is intended to provide wireless users with the same level of privacy as users in a wired network environment.

Public wireless connections such as hotspots can be somewhat insecure. (Hotspots are public or private areas where a wireless access point is available. For example, this wireless connection can be located at a library or coffee house.)

Temporal Key Integrity Protocol (TKIP) technology improves WEP by using a per-packet key mechanism, in which the base key is modified for each packet sent over the network. The overall key length is extended to 256 bits for encryption.

To obtain device-specific instructions on how to create, change, and start a VPN connection using your HP iPAQ, refer to the documentation that came with your device.

To get specific information about turning on or off WLAN and Wi-Fi, refer to the documentation on the *Companion* CD or *Getting Started* CD that came with your device.

Wi-Fi Protected Access (WPA) and TKIP/AES

Wi-Fi Protected Access (WPA) works with 802.11, and it secures a wireless network environment. WPA is intended to replace the current, less secure WEP system which is part of the Electrical and Electronic Engineers (IEEE) 802.11i standard.

WPA technology enables a practical, economical solution to wireless LAN security. WPA is also a strong encryption solution for wireless network security—especially while users roam from access point to access point.

A wireless network is a group of computers and associated devices that share a common wireless communication link over radio waves. A wireless network is enabled by a collection of wireless access points residing within a small geographic area, such as in an office building or wireless fidelity (Wi-Fi) public hotspot.

WLANs enable a variety of mobile transactions such as Internet and e-mail access, and sophisticated tasks such as allowing sales people to access customer records from customer locations.

TKIP/AES enhance the encryption methods of the 802.11 standards of WPA. These enhancements include:

- Improved data encryption for WPA (It provides more secured data encryption then WEP.)
- WPA allows simpler passphrases, based on preconfigured WEP keys (If you configure a passphrase for your access points, you cannot use 802.1x-based authentication. You must also use the same passphrase in Odyssey Client.)

Wireless fidelity (Wi-Fi)

Wi-Fi, also known as 802.11, is a communication standard created by the Institute of Electrical and Electronic Engineers (IEEE). The 802.11 standard defines the electrical and radio frequency components of a wireless Ethernet.

This standard also defines an encryption algorithm (Wired Equivalent Privacy, or WEP) to secure the network. The Wi-Fi Alliance is the body that ensures compatibility and is responsible for issuing standard compliance tests and logos.

Wi-Fi hotspots

Wi-Fi hotspots are WLANs that use the IEEE 802.11 protocol to establish wireless connections for general public use. Offered to customers by a growing number of hotels, restaurants, airport lounges, coffee shops and other businesses, Wi-Fi hotspots enable users to access Internet resources, send and receive e-mail, use instant messaging, and perform similar tasks they would otherwise perform on their business or home PCs. Before trying to connect to a wireless network at a public Wi-Fi hotspot, it is a good idea to find out what setting information you will need to connect to their network. Many Wi-Fi hotspots charge their customers a fee for this service.

Convenience and increased productivity make Wi-Fi hotspots attractive to users on the go, but hotspots can also increase the possibility of security risks. The security risks are manageable; however, if safety precautions are taken.

You can find out more information about Wi-Fi features and connections in the documentation on the *Companion* CD or *Getting Started* CD that came with your HP iPAQ.

WLAN standards

IEEE wireless standards such as 802.11 have undergone many improvements and addendums since they were first defined. The following list offers a high-level description of each of the better known standards:

- 802.11, which operates in the 2.4-GHz frequency band and offers only 2 megabits per second (Mbit/s) of overall throughput, was the original implemented standard.
- 802.11b is the most widely used form of Wi-Fi today. The radio operates within the 2.4-Ghz frequency band but allows a maximum data throughput of 11 Mbit/s.
- 802.11a is a short-range, but extremely high-speed, Wi-Fi network. This standard is not compatible with existing 802.11b networks. This high-speed Wi-Fi network operates in the 5-Ghz frequency band and can transfer data at a maximum speed of 54 Mbit/s.
- 802.11g is compatible with existing 802.11b networks, but also enables higher speeds. Its maximum speed is 54 Mbit/s, but 802.11g operates in the 2.4-Ghz frequency band.

Note: The 54-Mbit/s maximum speed of 802.11g is obtained only when the network contains other 802.11g-based devices. Users who mix 802.11b devices in that network will see a maximum throughput value of only 22 Mbit/s.

- The 802.1x standard defines the method of encapsulating EAPs over wired or wireless Ethernet networks. This standard does not define any specific security protocol, but is based on EAP types documented and ratified by the Internet Engineering Task Force (IETF).

Additional Security Solutions

Personal firewalls are the best way to protect your computer-related devices and wireless network. A firewall keeps computer hackers out and your sensitive data in; it acts as a barrier through which all information passes between the computer and the network. Personal firewalls monitor all incoming and outgoing traffic on your computer, including external systems.

Firewalls look at this data and make an access decision based on predetermined access rules. A firewall can give you the needed tools to protect your sensitive information while you're communicating across public networks. You have an option of selecting what information you want to protect, such as credit card numbers or passwords.

Personal firewalls can also prevent Web servers from getting access to sensitive data, and they can block Java applets and ActiveX controls. These Internet tools can endanger computer security. Firewalls can provide you with various helpful security needs for your computer hardware and software.

Personal firewalls are also available for mobile devices, such as Zone Alarm Personal Edition from Zone Labs, Inc. To download a free copy of this software on to your personal computer or notebook, go to www.zonelabs.com for more information.

Bluefire Security Technologies™ develops software that protects devices, data, and networks. The security solutions help prevent intrusion, provide integrity management, encryption, and authentication enterprise security. These security features add extra protection across VPNs, such as protecting lost and stolen devices; and preventing computer-hacker attacks and unauthorized access. Bluefire Mobile Firewall provides protection of information with encryption of data files, external storage cards, and personal information such as your mailbox, contact, calendar, and task databases. By visiting www.bluefiresecurity.com, Windows Mobile 2003 and Windows Mobile 5.0 users can download a free 30-day trial version of the software.

Pointsec® for Pocket PC provides convenient, real-time encryption of information on mobile devices as well as external storage cards. User-information is automatically encrypted and stored on your device. Pointsec for Pocket PCs is a pictured-based application. It is combined with PicturePIN® (access control) and QuickPIN® to provide fast re-entry to the device and its content. This security solution protects sensitive information in any format including Word Mobile, Excel Mobile, Outlook e-mail, attachments and notes. Your information is secure and instantly accessible. Pointsec® for Pocket PC is an integrated mobile security solution that provides users with strong encryption and fast, reliable speed or performance. You can learn more about security solutions that protect lost or stolen mobile devices by visiting www.pointsec.com.

These technologies can protect against unauthorized accesses, enforce security policies as well as monitor activity on devices.

Terminology

A glossary of security-related terms:

Acronym	Term	Definition
802.11b		The standard specification for wireless local area networks (WLAN), often called Wi-Fi.
802.1x		802.1x uses the protocol EAP (Extensible Authentication Protocol) to perform authentication when using a wireless network.
AES	Advanced Encryption Standard	A 128-bit block data encryption technique.
EAP	Extensible Authentication Protocol	A framework for transporting authentication protocols to secure networks: EAP-TTLS, EAP-PEAP, EAP-TLS, and EAP-LEAP.
Encryption (WEP) EAP or IEEE 802.1x		A set of security services used to protect 802.11 networks from unauthorized access.
SSID	Service Set Identifier	A sequence of characters that uniquely identifies a Wi-Fi network. (This identification number uses a maximum number of 32 characters and is case sensitive.).
TKIP/AES	Temporal Key Integrity Protocol	Improved data encryption for WPA. TKIP provides stronger encryption than WEP.
VPN	Virtual Private Network	A way of providing users (for example, remote offices, telecommuters, etc.) secure access to their organization’s network by way of the Internet.
WAP	Wireless Access Point	Physical hardware or computer software that acts as a hub for users of wireless devices to connect to a local area network (LAN).
WEP	Wired Equivalent Privacy	A security protocol designed to provide a wireless local area network (WLAN).
WLAN	Wireless Local Area Network	WLAN is a wireless network in which a mobile user can connect to a local area network through a wireless connection.
WPA	Wi-Fi Protected Area	WPA works with 802.11 standard, and it secures a wireless network environment.

For more information

iPAQ Mobile

http://www.hp.com/go/iPAQ

http://hp.com/sbso/wireless/index.html

MSN Mobile

http://www.mobile.msn.com/pocketpc

Call to action

www.hp.com

http://welcome.hp.com/country/us/en/support.html

www.hp.com/sbso/wireless/secure_wlan_mobile.pdf

www.bluefiresecurity.com

www.funk.com

www.microsoft.com/athome/security/default.mspx

www.microsoft.com/atwork/default.mspx

www.pointsec.com

www.zonelabs.com

5983-1105ENUC, 04/2006